Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Federación de Identidad aplicada a la autenticación de aplicaciones entre organizaciones

Autor: Ing. Andrés Jadán.
Tutor: Ing. Hugo Pagola

COHORTE 2013

Contenido

1.-Marco teórico

En la actualidad con el gran índice de uso de la tecnología en la mayoría de los aspectos de la vida diaria se ha generado el concepto de identidad digital, que se refiere a como las personas son identificadas dentro del mundo digital haciendo uso de credenciales como nombre de usuario o contraseña, las que pueden ser creadas por el mismo usuario o concedidas por una tercera parte.[1][2]

Para las empresas es muy importante el manejo de la identidad de sus colaboradores debido a que ellos son los que llevan a cabo las actividades que generan valor para el negocio y es necesario asegurarse que los recursos tecnológicos sean usados solamente para sus fines establecidos y por los usuarios autorizados, para así evitar que se generen perjuicios para las empresas.

El escenario común en el control de identidad en una empresa es en el que existe un controlador de dominio que se encarga de controlar el acceso a las estaciones de trabajo y en algunos casos al correo electrónico, pero para el acceso a las aplicaciones es manejado por cada una lo cual obliga al usuario a manejar varios tipos de credenciales y hacer uso de los mismos según el recurso que desee usar.

El escenario descrito además de dificultar las actividades de los usuarios genera costos elevados en la gestión de usuario ya que son necesarios más recursos para el manejo de los mismos. También se pueden generar vulnerabilidades debido a un deficiente cuidado en las claves por parte de los usuarios.

La solución que se encuentra disponible para optimizar este proceso es la federación de identidad que provee una forma de realizar un manejo centralizado de los usuarios reduciendo los costos y mejorando la seguridad en la gestión de la identidad.

1.1.-Conceptos básicos de la Federación de Identidad

"Federación de Identidad es federar la identidad de una entidad para facilitar el single sign on o el single log out a través de dominios distintos. Es un acercamiento a la autenticación de usuarios en varios sitios dentro de la misma compañía (Intranet) o en dominios independientes o dispares (extranet) haciendo uso de estándares abiertos".[3]

La federación de identidad permite que la autenticación de todas las aplicaciones existentes en una empresa sea llevada a cabo por una única entidad reduciendo los recursos necesarios para la administración y permitiendo que el usuario maneje un único par de usuario y contraseña.

El concepto del single sign on presentado se refiere a la funcionalidad implementada mediante la federación de identidad en la cual el usuario presenta sus credenciales una sola vez y este es autenticado en múltiples aplicaciones sin solicitarle nuevamente información de acceso.[4]

En una implementación de identidad podemos distinguir los siguientes elementos básicos:

a) **Repositorio de Usuarios:** Para poder realizar la autenticación de los usuarios es necesario que su información se encuentre guardada en un lugar seguro y confiable por ejemplo Active Directory.[5]
b) **Proveedor de Identidad:** Dentro de la implementación de federación de identidad es el elemento encargado de proveer la autenticación

accediendo a la información en el repositorio de usuarios y generando las credenciales necesarias para cada aplicación.[3]

c) **Proveedor de Servicio:** Los proveedores de servicio son los servidores en los que se encuentran disponibles las aplicaciones accedidas por los usuarios y que reciben las credenciales provistas por el proveedor de identidad para otorgar o denegar el acceso al recurso.

1.2.-Descripción de un esquema de Federación de Identidad

Un esquema de federación de identidad dentro de un único dominio estará compuesto por los elementos básicos antes mencionados: Repositorio de Usuarios, Proveedor de Identidad y un Proveedor de servicio, además del usuario que será el que inicie el proceso solicitando el acceso a un recurso.

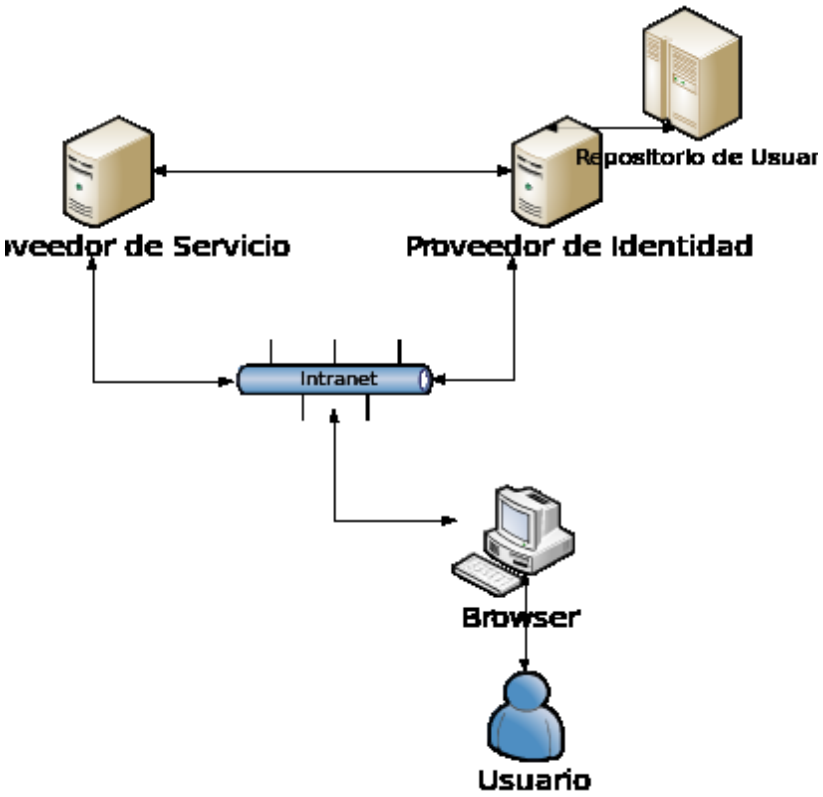


Ilustración 1 - Esquema de Federación de Identidad

En una implementación básica como la representada en la ilustración, la federación de identidad abarca a todos los recursos de una empresa que se encuentren dentro de la intranet corporativa con un proveedor de identidad que será el encargado de realizar la autenticación de los usuarios y de generar las credenciales necesarias para la autorización de los usuarios dentro de las aplicaciones.

1.2.1.-Autenticación Iniciada por el proveedor del Servicio

El acceso a los recursos se puede hacer de dos maneras dependiendo cual sea el elemento que inicia el proceso, el primer caso es el iniciado por el proveedor del servicio de la siguiente manera[6]:

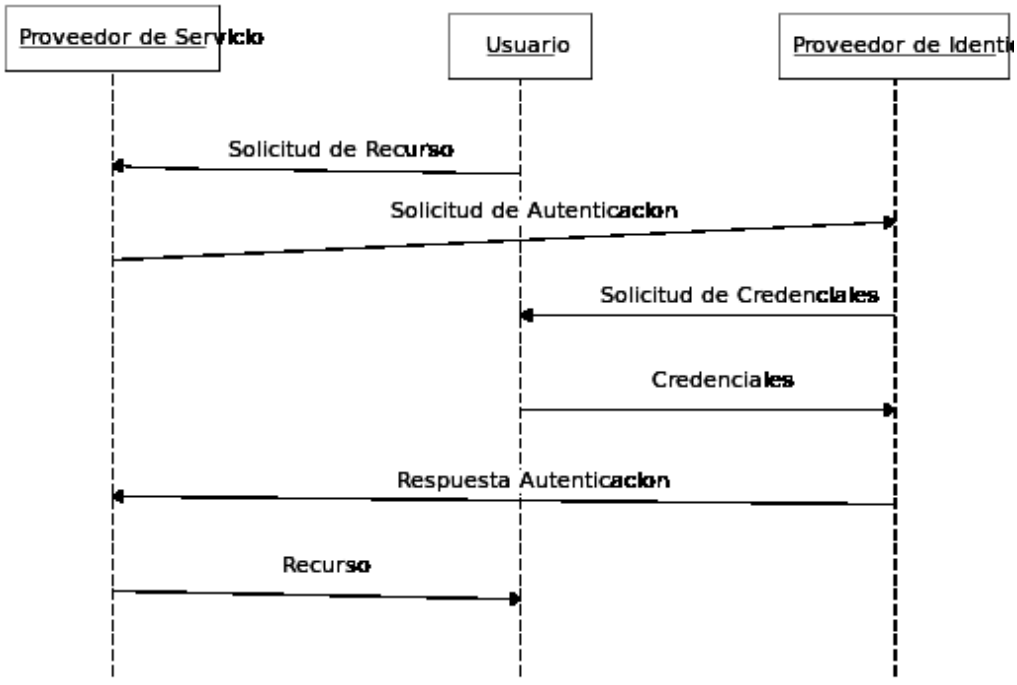


Ilustración 2 - Acceso iniciado por el proveedor del servicio

El proveedor del servicio recibe la solicitud de acceso a un recurso de parte del usuario, para poder autorizar el acceso solicita la autenticación del usuario al proveedor de identidad que se encarga del proceso generando las credenciales necesarias para la aplicación, una vez que el usuario ha sido autenticado el proveedor de servicio le otorgara acceso al recurso solicitado.

1.2.2.-Autenticación iniciada por el proveedor de identidad

El proceso de acceso al recurso también puede ser iniciado por el proveedor de identidad, en este proceso el usuario solicita autenticarse al proveedor de identidad, una vez autenticado se le presenta al usuario los recursos disponibles, con la elección del usuario el proveedor de identidad se comunica con el proveedor de servicio seleccionado.

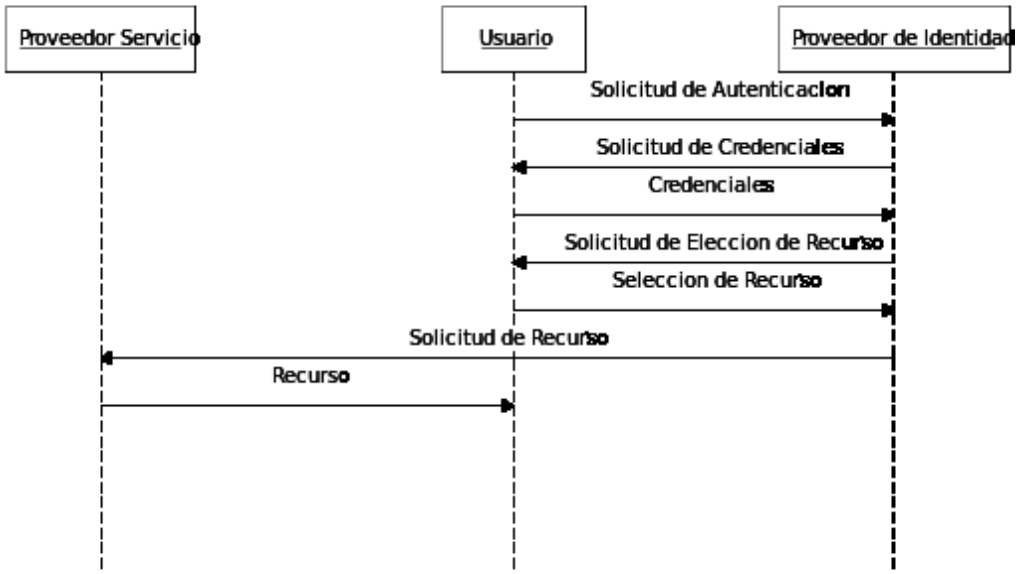


Ilustración 3 - Acceso iniciado por el Proveedor de Identidad

2.-Protocolos de Federación de Identidad

2.1.-SAML

SAML (Security AssertionMarkupLanguage) es un protocolo basado en XML que permite a los usuarios ingresar a varios sitios con una sola credencial es un esquema de federación de identidad.[6]

El protocolo SAML se basa en cuatro elementos básicos:[7]

2.1.1.-Assertions

Se definen como paquetes de información que contienen una o más sentencias generadas por una autoridad de autenticación, esta información puede ser de los siguientes tipos:

- **Autenticación:** Indica que el usuario ha sido autenticado para una aplicación en particular por un proveedor de identidad.
- **Atributos:** Un conjunto de atributos pertenecientes al usuario involucrado en el proceso de autenticación, son diferentes según los requisitos de la implementación.
- **Decisión de Autorización:** Indica si la petición de acceso a un recurso ha sido aceptada o rechazada.

2.1.2.-Protocolos

Se definen varios protocolos que son usados para la comunicación entre los diferentes elementos de una implementación que haga uso de SAML. Establecen la forma en la que el proveedor de servicio se comunicará con el proveedor de identidad para solicitar la autenticación de un usuario,

solicitar información adicional para el proceso de autorización además de establecer el mecanismo para el single log out.

2.1.3.-Enlaces

Es un mapeo de los intercambios de información en el proceso de intercambio de mensajes del tipo request-response, este mapeo es necesario para establecer la forma en la que serán enviados y recibidos los mensajes SAML dentro de paquetes SOAP o HTTP dependiendo del caso y del tipo de información.

2.1.4.-Perfiles

Los perfiles de SAML son usados para definir limitaciones o extensiones de sus funcionalidades para poder brindar soporte a determinadas aplicaciones o asegurar la interoperabilidad con otros protocolos o versiones anteriores.

2.2.-WS-Federation

WS-Federation es un protocol desarrollado por BEA Systems, BMC Software, CA Inc., IBM, Layer 7 Technologies, Microsoft, Novell, and VeriSign.

Este protocolo está basado en un marco base brindado por WS-Security, WS-Trust y WS-SecurityPolicy.

WS-Security implementa mecanismos para asegurar la autenticidad, integridad y confidencialidad de los mensajes intercambiados mediante el uso de tokens de seguridad, los cuales son descritos mediante WS-SecurityPolicy especificando el tipo de mensaje de seguridad que va a ser usado.[8]

WS-Trust complementa las funcionalidades mediante STS (SecuretokenService) que se encarga de compilar, firmar y emitir los tokens que serán usados por WS-Federation[9].

WS-Trust además define el protocolo usado para solicitar y enviar los tokens que son usados por WS-Security y que están definidos en WS-SecurityPolicy.

El protocolo definido por WS-Trust es independiente de la aplicación que los esté usando para solicitar, emitir o renovar un token de seguridad.
WS-Federation toma como base lo implementado en WS-Trust para generar las relaciones de confianza necesarias para establecer una federación de identidad y lo extiende para brindar las siguientes características.

2.2.1.-FederationMetadata

Cuando un servicio es compartido dentro de una federación de identidad es necesario también compartir la configuración para poder acceder al servicio WS-Federation implementa un modelo de metadata de federación que contiene esta información[8]:

2.2.2.-Autorización

Se puede realizar como una implementación especial del SecureTokenService en la que un proveedor del servicio especifica atributos adicionales para que se proceda a entregar el servicio. En este caso el encargado de la autorización es el proveedor de identidad.[8]

2.2.3.-Tipos de Autenticación

WS-Trust permite indicar el parámetro AuthenticationType en el que se define el tipo de autenticación solicitado por el servicio y el nivel de confianza de la misma.[8]

2.2.4.-Servicios de Atributos

En algunos casos el proveedor de servicios necesita información adicional para realizar la autorización de un usuario, para esto se implementa mecanismos de acceso a la información necesitada por medio de SecureTokenService.[8]

2.2.5.-Pseudónimos

El servicio de pseudónimos brinda al usuario una identidad alternativa para acceder a los recursos, esto se realiza mediante un servicio de pseudónimos que se encarga de asociar los tokens generados con los pseudónimos que pueden ser diferentes para cada servicio o dominio.[8]

2.2.6.-Privacidad

Extensiones al proceso de solicitud de tokens para que la parte interesada especifique sus necesidades de privacidad, se puede indicar la información que se considere sensible y deba ser protegida.[8]

2.2.6.-FederatedSignOut

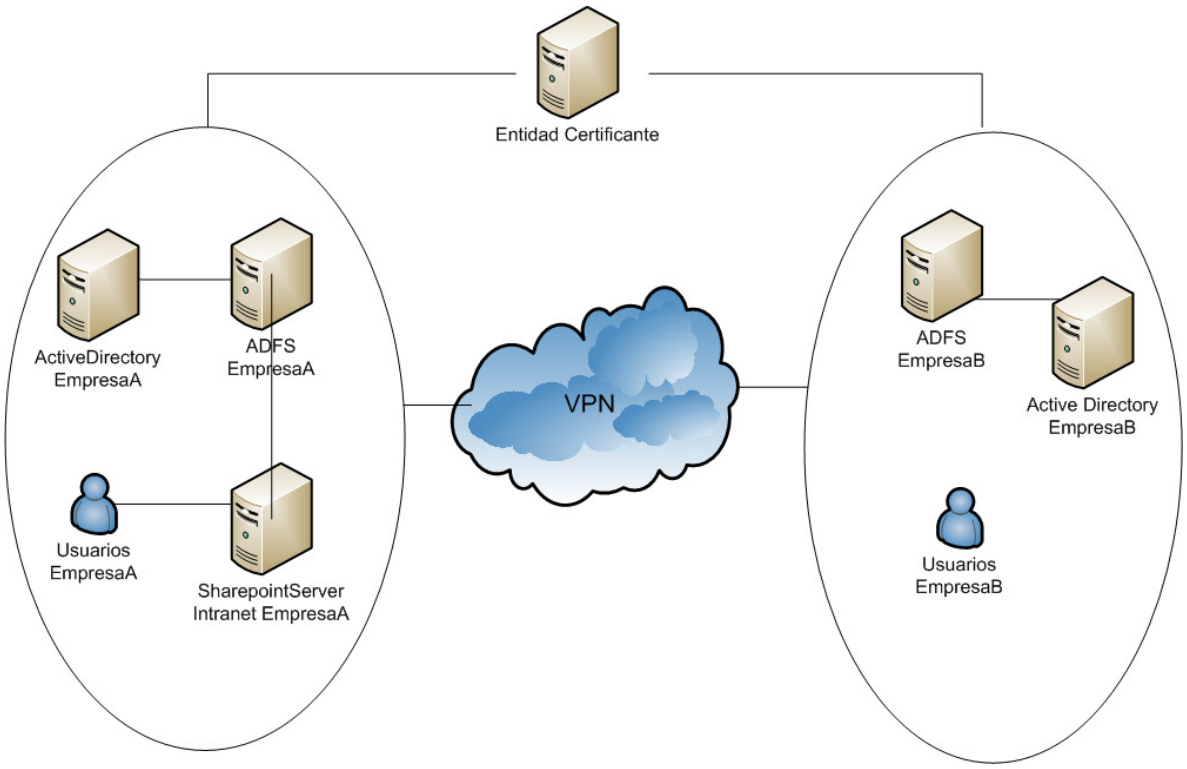
WS-Federation cuenta con un mecanismo mediante el cual se puede solicitar que se eliminen todas las sesiones activas o tokens activos cuando un usuario cierra su sesión.[8]

3.-Prueba de Concepto

3.1.-Descripción

Para la implementación de una prueba de concepto de la federación de identidad se ha elegido el siguiente escenario: Dos empresas llamadas EMPRESAA y EMPRESAB han comenzado un proyecto de colaboración. Para llevar a cabo el proyecto la EMPRESAA pone a disposición su sitio de intranet como repositorio de documentos.

Las dos empresas cuentan con dominios implementados en Active Directory en el que tienen registrados sus usuarios, decidiéndose que los usuarios ingresen al sitio de intranet de la EMPRESAA con las credenciales que manejan en sus respectivos lugares de trabajo.



En el esquema anterior se muestra la arquitectura de la implementación en la que los servidores de dominio de ambas empresas serán Active Directory sobre un sistema operativo Windows server 2008 y los usuarios de ambas empresas trabajan en un ambiente con sistema operativo Windows 7.Para realizar la autenticación de usuarios en la intranet se hará uso del servidor de federación Active Directory Federation Services, cada una de las empresas contará con un servidor de federación ADFS sobre un sistema operativo Windows server 2008.

Como servidor de recursos se usará un servidor Microsoft Office Sharepoint Server 2007 que será configurado para aceptar las credenciales generadas por los servidores que actúan como proveedores de identidad.

También se incluye dentro de la infraestructura un servidor que funcionara como entidad certificante, para esto se utilizara un servidor Windows server 2008 con los servicios de servidor instalados.

3.2.-Implementación

La prueba de concepto se llevo a cabo utilizando maquinas virtuales sobre la plataforma vmware versión 10.

Previo a realizar las configuraciones para el funcionamiento de la federación de identidad los servidores virtuales fueron preparados de la siguiente manera

- Servidores de Dominio
    - Dominio EmpresaA
        - Nombre: ADEMPRESAA
        - Dominio: empresaa.com.ar
        - Sistema Operativo: Windows Server 2008 R2

        - Servicios Instalados
            - Active Directory Domain Services
            - DNS
            - IIS
        - IP: 192.168.0.100
    - Dominio EmpresaB
        - Nombre: ADEMPRESAB
        - Dominio: empresab.com.ar
        - Sistema Operativo: Windows Server 2008 R2
        - Servicios Instalados
            - Active Directory Domain Services
            - DNS
            - IIS
        - IP: 192.168.0.200
- Servidor Web
    - Nombre: INTRANET
    - Dominio: adempresaa.com.ar
    - Sistema Operativo: Windows Server 2003 Enterprise Service Pack 2
    - IIS (habilitado ASP.NET 2.0)
    - Microsoft Office SharePoint 2007 (Se uso esta versión ya que consume menos recursos)
- Certificados Digitales
    - Para la emisión de los certificados se utilizo los servicios de certificación de Windows server generando certificados para cada servidor con una llave RSA 1024.
    - Cada equipo tendrá instalado su certificado digital y el de los demás equipos en los repositorios correspondientes.
    - Instalar el certificado de la Entidad Certificante en el repositorio TRUSTED CERTIFICATION AUTHORITIES.
- DNS

- Se debe agregar una zona de búsqueda para resolver los nombres de los equipos del dominio externo.
- Zona de búsqueda reversa, necesario para la correcta comunicación durante el proceso de solicitud/emisión de tokens.

Para los servidores de identidad se uso Active Directory Federation Services en su versión 2.0, para la prueba de concepto se instalara este servicio en el servidor de dominio de cada empresa, en una implementación real debe ser instalado en servidores separados.

Durante la instalación del servidor de identidad se debe especificar que se creara un nuevo bosque de servidores de identidad en el cual el nuevo servidor será el primario.

El servidor de identidad de cada una de las organizaciones actuara por separado y tomara como repositorio de usuarios al active directory correspondiente a su organización.

En el servidor Web Sharepoint 2007 que actuara como proveedor de recursos se ha creado un sitio para compartir documentos, se accederá al sitio mediante protocolo SSL con la siguiente dirección:

https://intranet.empresaa.com.ar.

Para que el servidor web pueda aceptar los tokens generados por el servidor de identidad se instalara la herramienta Federation Utility for SharePoint 3.0.

Esta herramienta configurara la aplicación indicada para que acepte los tokens generados por el servidor de identidad, por una parte anexara al archivo web.config la siguiente línea.

<add key="FederationMetadataLocation" value="https://adempresaa.empresaa.com.ar/FederationMetadata/2007-06/FederationMetadata.xml" />

En la que se indica la dirección del servidor de identidad que será usado para la aplicación.

La aplicación también creara el archivo de metadata necesaria para indicar al servidor de identidad el contenido esperado de los tokens de la siguiente manera.

<auth:ClaimType Uri="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" />

<auth:ClaimType Uri="http://schemas.microsoft.com/ws/2008/06/identity/claims/role" Optional="true" xmlns:auth="http://docs.oasis-open.org/wsfed/authorization/200706" />

En las etiquetas anteriores se definen los atributos esperados de parte del servidor de identidad, estos atributos son elegidos de un conjunto que contiene toda la información disponible en el active directory de una empresa.

La información de la metadata del sitio deberá ser accedida por el servidor de identidad para poder formar los tokens, esta información se publicara en la siguiente dirección:

https://intranet.empresaa.com.ar/_LAYOUTS/images/443/federationmetadata/2007-06/federationmetadata.xml.

En el servidor de identidad es necesario crear la relación de confianza con el servidor de recursos, esto se realizara en el servidor de identidad en la zona llamada Relying Party Trust.

Para completar la configuración de esta relación de confianza se establece la manera en la que se comunicaran los atributos al servidor de recursos.

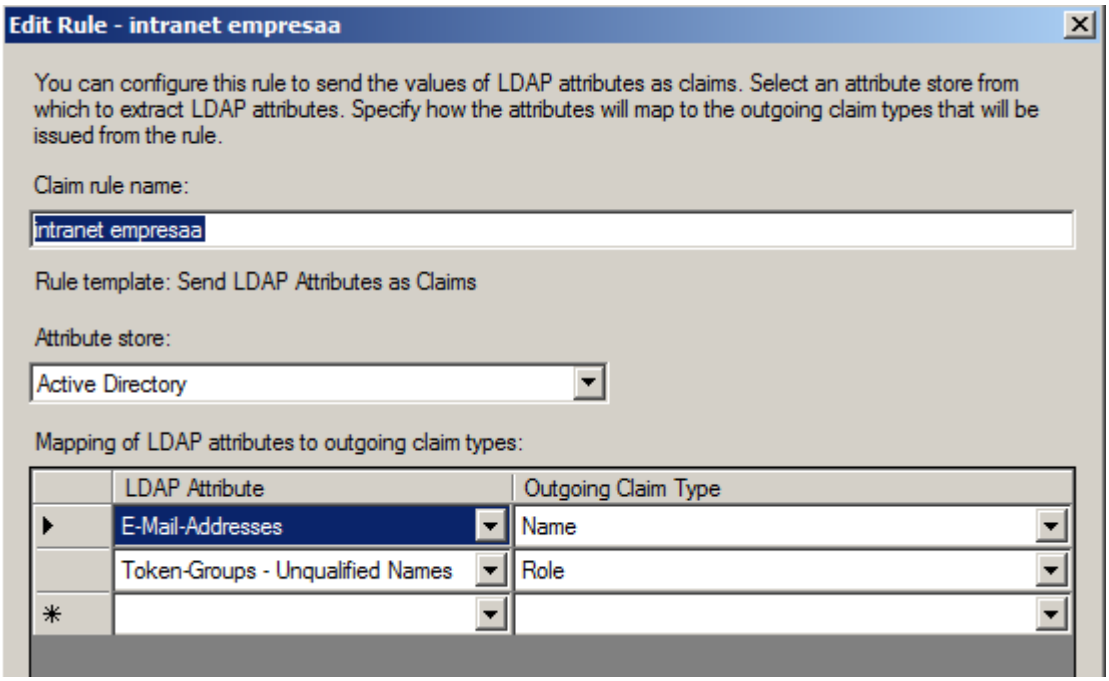


Ilustración 4 - Configuración reglas ADFS EMPRESAA

En la imagen anterior se puede ver la configuración de los atributos que serán enviados al proveedor de recursos, en este caso se han especificado dos atributos por parte del proveedor de recursos (Name, Role)

Para el atributo Name se indica que será enviada la dirección de correo completa del usuario con la finalidad de identificar el nombre del usuario y el dominio al que pertenece de la forma *usuario1@empresaa.com.ar*.

Para el atributo Role requerido por el servidor de recursos se utilizara el nombre del grupo al que pertenezca el usuario, en este caso solamente los usuarios que pertenezcan al grupo Intranet podrán tener acceso al recurso.

Una vez realizadas estas configuraciones cuando se acceda al sitio SSL de la intranet de la EMPRESAA el sitio se redirigirá a un formulario de login provisto por el servidor de identidad.

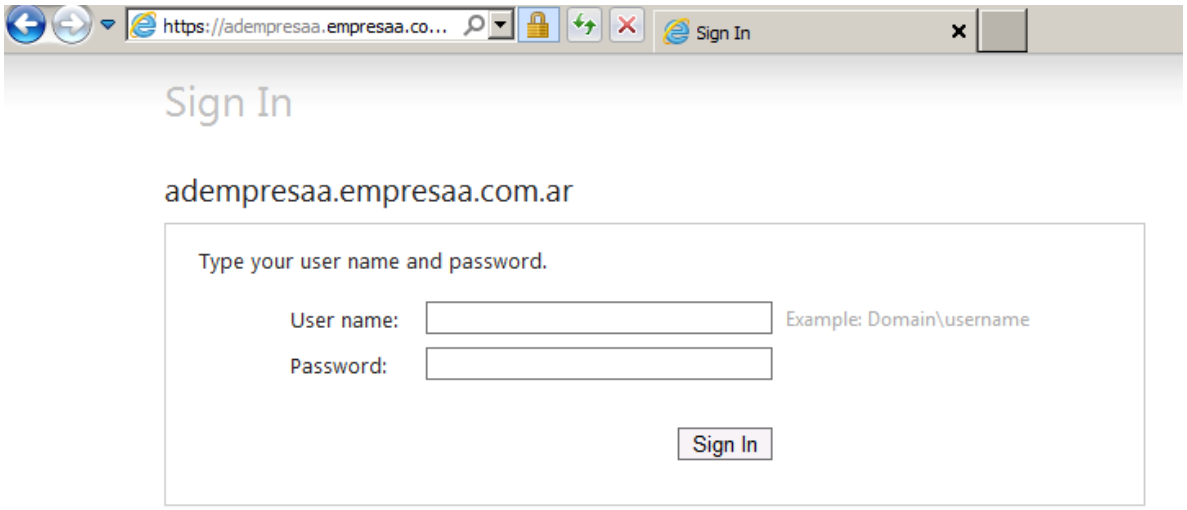


Ilustración 5 - Interfaz login servidor ADFS

Con esto se completara el proceso de log in y el servidor de recursos autorizara a los usuarios que pertenezcan al grupo Intranet y se les presentara la página de inicio del sitio.

Para que los usuarios del dominio EMPRESAB puedan acceder al sitio se configurara la relación de confianza entre los dos servidores de identidad.

Se agrego al servidor de identidad de la EMPRESAB en la zona de Claims Provider Trusts en la cual se encuentran los servidores que proveen la autenticación de usuarios, en esta zona se encuentra por defecto el active directory del dominio.

Al agregar la nueva relación se puede configurar la forma en la que serán recibidos los atributos del proveedor, en este caso se configuro un filtro para el atributo de dirección de correo electrónico para permitir solamente direcciones que pertenezcan al dominio empresab.com.ar

Para finalizar en el servidor de identidad de EMPRESAB se debe agregar al servidor de identidad de EMPRESAA en la zona de Relying Party Trust.

La relación de confianza establecida permite que el servidor de identidad de EMPRESAB se encargue del proceso de autenticación de los usuarios de su dominio y comunique los atributos especificados al servidor de identidad de EMPRESAA que solamente se encargara de pasar estos atributos al servidor de recursos que se encuentra en su dominio.

4.-Requerimientos Funcionales y Operativos

En cualquier sistema se debe identificar claramente los elementos claves en los que se debe asegurar un nivel de servicio específico de acuerdo a las necesidades de las organizaciones, en el caso de la federación de identidad los elementos más importantes son el proveedor de recursos y el proveedor de identidad.

En el caso de los servidores que actúen como proveedores de recursos el nivel de disponibilidad dependerá de cada organización la que definirá estos niveles de acuerdo a sus necesidades.

Se debe tener en cuenta la disponibilidad y correcto funcionamiento del canal de comunicación entre el proveedor de recursos y el proveedor de identidad.

Para proveedores de recursos que contengan aplicaciones claves para el negocio se deberá contar con conexiones alternativas en caso de fallar las principales.

El proveedor de identidad está compuesto por dos elementos: el servidor que contiene los servicios de federación y el servidor que contiene el repositorio de usuarios del dominio.

El repositorio de usuarios o servidor de dominio debe estar disponible siempre que sea necesario realizar la autenticación de un usuario dentro de la federación.

Para asegurar la disponibilidad se debe implementar un servidor de dominio secundario configurado de manera que refleje todos los cambios realizados en el servidor primario y que pueda ser accedido en caso de no encontrarse disponible el servidor primario.

Es recomendable separar el servicio de federación a un servidor independiente para asegurar la disponibilidad en caso de falla del servidor de dominio primario.

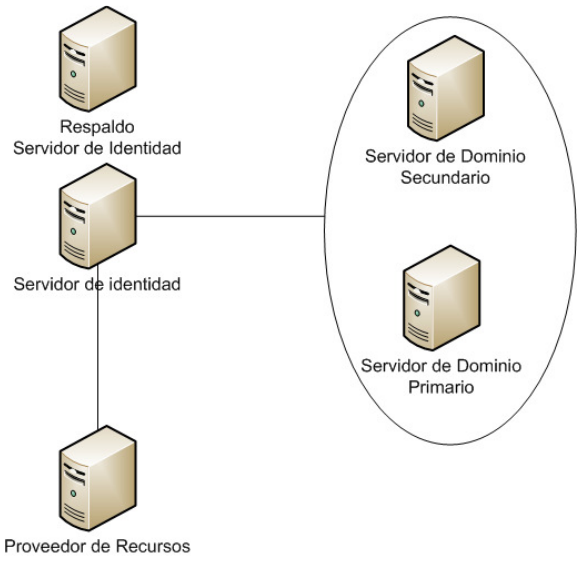


Ilustración 6 - Esquema de Federación de Identidad Sugerido

La figura anterior muestra la arquitectura recomendada para una implementación de federación de identidad de alta disponibilidad, con dos servidores de dominio, uno primario y otro secundario que funcionará como repositorio de usuarios de forma transparente para el proveedor de identidad.

En la arquitectura se incluye un servidor de respaldo del proveedor de identidad, el cual debe contener las mismas configuraciones que el servidor primario y encontrarse listo para funcionar en caso de falla. En caso de no poder contar con un servidor de respaldo idéntico al principal se deberá

realizar copias de seguridad de todas las configuraciones del proveedor de identidad.

5.-Requerimientos de Seguridad

En un esquema de federación de identidad es muy importante la correcta autenticación de los usuarios que tienen acceso a los recursos que se están compartiendo y el acceso indebido a estos recursos, que puede generar daños a la organización.

5.1.-Seguridad de Contraseñas

El primer punto que tenemos que considerar es la seguridad de las contraseñas, dentro de los repositorios de usuarios cada usuario estará relacionado con una contraseña que debe ser suficientemente robusta para que no sea fácil adivinarla y que sea resistente a ataques de fuerza bruta.

La fortaleza de una contraseña se basa en su longitud y complejidad como lo indica la NIST en su publicación especial “800-118 Guide to Enterprise Password Management”, la contraseña será más resistente a ataques según se aumente su longitud y se añadan set de caracteres permitidos para su formación.[10]

Si bien la seguridad de la contraseña aumenta con la complejidad, hay que tomar en cuenta lo dificultoso que puede resultar para el usuario manejar una contraseña demasiado compleja, lo recomendable es establecer una norma que sea manejable y fácil de memorizar para el usuario.

También hay que tomar en cuenta regulaciones de organismos externos como es el caso del banco central de la república Argentina que en una de sus comunicaciones establece que la longitud mínima de las contraseñas será de 8 caracteres y el almacenamiento de un historial de las ultimas 12 contraseñas usadas para que no puedan volver a ser usadas.[11]

5.2.-Seguridad de los Servidores

Los servidores que son parte de la implementación deben de ser protegidos de forma física y lógica. Físicamente tienen que estar ubicados en un ambiente seguro para su funcionamiento.

De manera lógica los servidores tienen que ser protegidos mediante un firewall ya que se encuentran expuestos a una red externa al compartir sus recursos.

Para asegurar la integridad de la red interna de cada una de las empresas se debe separar los servidores que se encuentren expuestos a la red externa para esto se debe implementar una DMZ para estos servidores.

Se debe implementar un esquema de respaldos sobre la configuración y la información contenida dentro de los servidores, de manera que se pueda levantar nuevos servidores en caso de pérdida de los servidores de producción.

5.3.-Auditoria

Debido a que se está compartiendo un recurso con una empresa externa es necesario llevar un registro de los usuarios que acceden al recurso y sus actividades.

En la federación de identidad se debe llevar este registro en el proveedor de identidad y en el proveedor de recursos. En el registro realizado por el proveedor de servicio es necesario especificar la información de usuario necesaria al proveedor de identidad. La información básica recomendada es la siguiente:

- Id de usuario.

- Dominio
- Organización
- Grupo al que pertenece

El proveedor del recursos es el encargado de complementar esta información con información sobre la hora y fecha de acceso y las actividades que ha realizado el usuario, también se debe registrar el id del proveedor de identidad que ha autenticado al usuario, y de manera opcional se puede almacenar el token de seguridad entregado por el usuario.

En el proveedor de identidad se lleva a cabo el registro de los incidentes de seguridad en cuanto al funcionamiento del servidor, registrándose los posibles errores que hayan ocurrido en su funcionamiento.

Para poder asegurar la trazabilidad de los registros de auditoría es necesario poder relacionar los registros mediante su hora y fecha, para que esto sea posible es necesario implementar un time server para sincronizar los servidores. Esta implementación se debe de llevar a cabo en conjunto con todas las organizaciones que participen de la federación.

Hay que tener en cuenta también la funcionalidad que brinda la federación de identidad para el uso de pseudónimos lo cual esta implementado para asegurar la privacidad de los usuarios, pero en el caso de organizaciones se debe evitar su uso ya que de ser así no se podría llevar un adecuado registro de las actividades de los usuarios.

5.4.-Intercambio de Información

La comunicación entre el proveedor de recursos y el proveedor de identidad puede ser realizada mediante el browser web, este tipo de comunicación

expone al servicio a la vulnerabilidad “man in the middle”, ya que los paquetes pueden ser capturados por una tercera parte.

Para evitar esto se recomienda el uso de la modalidad de comunicación “back channel”, en la que la comunicación, de ser necesario información o alguna acción del usuario, se realiza directamente entre el proveedor de identidad y el proveedor de recursos solamente usando el browser..

También es necesario asegurar el vínculo que comunica a las dos o más organizaciones que conforman la federación, para lo cual se recomienda que toda la comunicación se realice mediante un canal seguro, como por ejemplo una conexión VPN.

Toda comunicación se debe realizar mediante el protocolo SSL para esto es necesario que todos los servidores involucrados cuenten con un certificado digital.

Los certificados digitales utilizados para la comunicación SSL también serán usados para la encriptación de las credenciales generadas por los servidores de identidad, se recomienda el uso de certificados con una clave RSA de 1024 bits.

6.-Catalogo de Recomendaciones

Como resultado del relevamiento de información teórica sobre la federación de identidad y de la implementación de la prueba de concepto se ha obtenido como resultado un conjunto de recomendaciones que se presentan en los siguientes catalogos.

6.1.-Catalogo de Recomendaciones Funcionales

6.1.1.-Proveedor de Identidad

RF-PI-01	**Repositorio de Usuarios** La implementación debe contar con un repositorio para almacenar los usuarios por ejemplo: Active Directory, LDAP.
RF-PI-02	**Comunicaciones** Un canal de comunicaciones seguro y redundante para la red interna y una conexión segura y cifrada para la red externa por ejemplo VPN.
RF-PI-03	**Certificados Digitales** Necesarios para generar los tokens, deben ser generados por una Autoridad Certificante de Confianza y según los estándares de seguridad.

6.1.2.-Proveedor de Servicio

RF-PS-01	**Protocolo Federación** Las aplicaciones instaladas dentro del servidor de servicios deberán ser compatibles con alguno de los protocolos de federación de identidad.
RF-PS-02	**Comunicaciones** Un canal de comunicaciones seguro y redundante para la red interna y una conexión segura y cifrada para la red externa por ejemplo VPN.
RF-PI-03	**Certificados Digitales** El acceso a los recursos o servicios que presenta el servidor se deberá realizar por el protocolo SSL por lo que debe contar con los certificados necesario instalados.

6.2.-Catalogo de Recomendaciones Operativas

6.2.1.-Servidor de identidad

RO-PI-01	**Repositorio de Usuarios** Para asegurar la disponibilidad del repositorio de usuarios se debe realizar una implementación con servidor primario y secundario.
RO-PI-02	**Comunicaciones** El canal de comunicaciones debe contar con un respaldo en caso de fallas para asegurar la disponibilidad del repositorio
RO-PI-03	**Separación de Servicio** Se debe separar el servicio de federación de identidad del repositorio a un servidor dedicado para optimizar el servicio
RO-PI-04	**Backups** Se recomienda un backup completo del repositorio de usuarios y un backup de las configuraciones del servidor de federación.

6.3.-Catalogo de Recomendaciones de Seguridad

6.3.1.-Proveedor de Identidad

RS-PI-01	**Seguridad Física** Todos los servidores tienen que estar ubicados en una sala adecuada que brinde un nivel seguridad adecuado a la criticidad del sistema.
RS-PI-02	**Contraseñas** Implementar recomendaciones de composición de contraseñas: NIST 800-118, Comunicaciones del Banco central de la república Argentina en el caso de instituciones financieras.
RS-PI-03	**Separación de la red Interna** El servidor deberá estar ubicado dentro de una DMZ ya q este expone servicios a una red externa.
RS-PI-04	**Backups** Se recomienda un backup completo del repositorio de usuarios y un backup de las configuraciones del

	servidor de federación.
RS-PI-05	**Auditoria Sistema Operativo** Se deben activar las opciones de auditoría del sistema operativo para registrar eventos irregulares (ingresos indebidos, errores del sistema, cambios en configuraciones).
RS-PI-06	**Auditoria Servicio de Federación** Registrar eventos de cambio de configuración de las reglas de autenticación.
RS-PI-07	**Configuración Horaria** Para asegurar la trazabilidad se debe configurar correctamente la hora y fecha en todos los servidores y de ser posible implementar un time server
RS-PI-08	**Auditoria Usuarios** Para que el proveedor realice la auditoria de acceso a los recursos se debe entregar como mínimo los siguientes atributos: Id de usuario, Dominio, Organización, Grupo al que pertenece.
RS-PI-09	**Certificados Digitales** Para asegurar la integridad de la comunicación se establece una conexión SSL para lo que se recomienda certificados digitales con clave RSA de 1024 bits
RS-PI-10	**Comunicación de Tokens** Usar el método back channel para evitar ataques man in the middle.

6.3.2.-Proveedor de Recursos

RS-PS-01	**Seguridad Física** Todos los servidores tienen que estar ubicados en una sala adecuada que brinde un nivel seguridad adecuado a la criticidad del sistema.
RS-PS-02	**Separación de la red Interna** El servidor deberá estar ubicado dentro de una DMZ ya q este expone servicios a una red externa.
RS-PS-03	**Backups** Dependerá de la criticidad del servicio dentro de la organización y de los recursos disponibles, se recomienda un respaldo completo a la semana y respaldos incrementales diarios.
RS-PS-04	**Disponibilidad** De acuerdo a las necesidades de la organización se establecerá el nivel a implementarse, para servicios críticos se recomienda una implementación de servidores en espejo para que en el caso de falla se

	pueda restablecer el servicio inmediatamente. En el caso de servicios no críticos se recomienda contar con un servidor con el sistema operativo instalado para poder replicar las configuraciones y datos del servidor original desde los respaldos.
RS-PS-05	**Auditoria Servicio** Cada servicio debe llevar un registro de los usuarios autenticados por el servidor de identidad guardando los atributos entregados, una marca de tiempo y de manera opcional almacenar el token de seguridad entregado.
RS-PI-06	**Configuración Horaria** Para asegurar la trazabilidad se debe configurar correctamente la hora y fecha en todos los servidores y de ser posible implementar un time server

6.3.3.-Canal de Comunicaciones

RS-CC-01	**Seguridad Física** Los equipos de comunicación deben encontrarse debidamente resguardados.
RS-CC-02	**Disponibilidad** Las conexiones con redes externas deben contar con un enlace alternativo en caso de falla.
RS-CC-03	**SSL** Todo servicio web deberá ser brindado a través del protocolo HTTPS en la versión más reciente.
RS-CC-04	**VPN** La comunicación con redes externas deberá realizarse mediante una canal VPN para evitar posibles intrusiones.

6.3.4 Usuario Final

RS-UF-01	**Contraseñas** El usuario no debe compartir su contraseña y asegurarse de seguir las recomendaciones de formación de contraseñas.
RS-UF-02	**SSL** Se debe verificar que todo acceso a recursos web sea mediante el protocolo HTTPS y que el explorador web

	detecte un certificado digital valido.
RS-UF-03	**Cierre de Sesión** Asegurarse de cerrar sesión en los servicios que ya no vayan a ser usados.
RS-UF-04	**Usuarios Corporativos** Implementar políticas de control sobre los equipos de los usuarios dentro del ámbito corporativo (Privilegios, Horario de acceso, Auditoria)

6.3.5 Políticas de Seguridad

RS-PS-01	**DRP** La organización debe contar con un Disaster Recovery Plan debidamente documentado y probado.
RS-PS-02	**Política de Backups** Establecer y documentar una política para la toma de Backups especificando la periodicidad y los encargados de realizar las operaciones
RS-PS-02	**Acceso a Recursos** Mantener claramente documentado los roles y funciones del personal autorizado a acceder a los recursos.
RS-PS-03	**Concientización** Concientizar a los usuarios internos y externos sobre el uso seguro de los sistemas informáticos.

7.-Conclusiones

En el desarrollo de este trabajo práctico se realizo un relevamiento de los principios básicos sobre la federación de identidad, describiendo su funcionamiento y realizando una breve descripción de los protocolos más usados en el mercado.

Para complementar el marco teórico se implemento una prueba de concepto en la que se replico un escenario de federación de identidad aplicado a dos organizaciones con dominios diferentes.

Al revisar los resultados de la prueba de concepto se puede concluir que la Federación de Identidad cumple con el objetivo de reducir la complejidad de la administración de los usuarios en los escenarios en los que se encuentren involucrados dos o más dominios.

Una organización que decida realizar esta implementación deberá realizar un análisis costo beneficio antes de su implementación debido a los requisitos de infraestructura que demanda esta solución.

La implementación requiere un trabajo conjunto de las organizaciones involucradas, este aspecto es el que potencialmente consumirá más recursos debido a todos los requerimientos técnicos de la implementación.

Las organizaciones deben tomar especial cuidado a todos los requisitos de seguridad debido a que todos los servidores involucrados en el proceso se encontraran expuestos a una red externa aumentando así el riesgo de posibles ataques que pueden comprometer la red interna de la organización.

Se han identificado diferentes requerimientos funcionales, operativos y de seguridad para una solución de este tipo, para cumplir con estos requisitos es necesario que las organizaciones lleven un análisis previo y posterior a la implementación verificando su cumplimiento.

Este trabajo se centra en el análisis de un esquema de autenticación obteniendo como resultado recomendaciones para la implementación del mismo, estos resultados dan pie para un trabajo de investigación más extenso incluyendo otros esquemas de autenticación usados en el mercado.

Bibliografía

[1] «Whatis a Digital Identity? - DefinitionfromTechopedia». [En línea]. Disponible en: http://www.techopedia.com/definition/23915/digital-identity. [Accedido: 19-ago-2014].
[2] «WhatIs Digital Identity?». [En línea]. Disponible en: http://www.wisegeek.com/what-is-digital-identity.htm. [Accedido: 19-ago-2014].
[3] «The fundamentals of identity federation». [En línea]. Disponible en: http://searchsoa.techtarget.com/tip/The-fundamentals-of-identity-federation. [Accedido: 19-ago-2014].
[4] «What is single sign-on (SSO)? - Definition from WhatIs.com».[En línea]. Disponible en: http://searchsecurity.techtarget.com/definition/single-sign-on. [Accedido: 19-ago-2014].
[5] «FIM_White_Paper_Identity_Federation_Concepts.pdf». .
[6] «What is SAML (Security Assertion Markup Language)? - Definition from WhatIs.com».[En línea]. Disponible en: http://searchfinancialsecurity.techtarget.com/definition/SAML. [Accedido: 16-sep-2014].
[7] «SAML XML.org | Online community for the Security Assertion Markup Language (SAML) OASIS Standard». [En línea]. Disponible en: http://saml.xml.org/. [Accedido: 16-sep-2014].
[8] «Understanding WS-Federation». [En línea].Disponible en: http://msdn.microsoft.com/en-us/library/bb498017.aspx. [Accedido: 17-oct-2014].
[9] «Security TokenService». [En línea]. Disponible en: http://msdn.microsoft.com/es-ar/library/ee748490.aspx. [Accedido: 05-nov-2014].
[10] «NIST SP 800-118, Guide to Enterprise Password Management (DRAFT) - draft-sp800-118.pdf». .
[11] «Aplicación de “Envío de Comunicaciones y Comunicados” - a4609.pdf». .